Chapter 10.
International Security Requirements

Section 1. General and Background Information

10-100. General. This Chapter provides policy and procedures governing the control of classified information in international programs. It also provides procedures for those aspects of the ITAR that require compliance with this Manual. (The terms used in this Chapter may differ from those in the ITAR). This Section contains information concerning the Federal laws and regulations, the National Disclosure Policy, and the international agreements that govern the disclosure of classified and other sensitive information to foreign interests.

10-101. Policy. The private use of classified information is not permitted except in furtherance of a lawful and authorized Government purpose. Government Agencies have appointed individuals to the positions of Principal and Designated Disclosure Authorities to oversee foreign disclosure decisions. These officials authorize the release of their agency's classified information that is involved in the export of articles and services. They determine that the release is essential to the accomplishment of the specified Government purpose; the information is releasable to the foreign government involved; and the information can and will be adequately protected by the recipient foreign government.

10-102. Applicable Federal Laws. The transfer of articles and services, and related technical data, to a foreign person, within or outside the U.S., or the movement of such material or information to any destination outside the legal jurisdiction of the U.S., constitutes an export. Depending on the nature of the articles or data, most exports are governed by the Arms Export Control Act, the Export Administration Act, and the Atomic Energy Act.

a. **The Arms Export Control Act (AECA) (22 U.S.C. 2751).** This Act governs the export of defense articles and services, and related technical data, that have been determined to constitute "arms, munitions, and implements of war," and have been so designated by incorporation in the U.S. Munitions List. The AECA is implemented by the Department of State (Office of Defense Trade Controls) in the ITAR (22 CFR 120 et seq.). Exports of classified defense articles and data on the U.S. Munitions List are also subject to the provisions of the National Disclosure Policy. The AECA requires agreement by foreign governments to protect U.S. defense articles and technical data provided to them.

b. **The Export Administration Act (EAA) (50 U.S.C. app. 2401 Note).** This Act governs the export of articles and technical data that are principally commercial in nature and deemed not appropriate for inclusion on the U.S. Munitions List. The EAA is implemented by the Department of Commerce (Bureau of Export Administration) in the Export Administration Regulation (15 CFR 368 et seq.). This Regulation establishes a list of commodities and related technical data known as the Commerce Control List. Some of these controlled commodities are referred to as "dual-use." That is, they have an actual or potential military as well as civilian, commercial application. Therefore, export of certain dual-use commodities requires DoD concurrence. Exports under the EAA do not include classified information. (NOTE: The EAA expired in 1990, but was revived in 1993 (P.L. 103-10); however, the administrative controls have been in continuous effect under E.O. 12730 of September 30, 1990, and now E.O. 12868 of September 30, 1993).

c. **The Atomic Energy Act (AEA) of 1954, as amended (42 U.S.C. 2011).** This Act provides a program of international cooperation to promote common defense and security, and makes available to cooperating nations the benefits of peaceful applications of atomic energy, as expanding technology and considerations of the common defense and security permit. RD and FRD may be shared with another nation only under the terms of an agreement for cooperation.

d. **The Defense Authorization Act of 1984 (10 U.S.C. 130).** This Act authorizes the Secretary of Defense to withhold from public disclosure unclassified technical data that has military or space application, is owned or controlled by the DoD, and is subject to license under the AECA or EAA. Canada has a similar law. A qualified contractor in the United States and Canada that is registered at the Joint Certification Office, Defense Logistics Agency, may have access to this technical data in support of a U.S. or Canadian Government requirement. A foreign contractor may have access to the U.S. technical data upon issuance of an export license or other written U.S. Government authorization, and their agreement to comply with requirements specified in the export authorization. The information that is subject to these additional controls is identified by an export control warning and distribution statements that describe who may have access and the reasons for control.

10-103. National Disclosure Policy (NDP). Decisions on the disclosure of classified military information to foreign interests, including classified information related to defense articles and services controlled by the ITAR, are governed by the NDP. U.S. Government policy is to avoid creating false impressions of its readiness to make available classified military information to foreign interests. The policy prescribes that commitments shall not be expressed or implied and there may be no disclosure of any information until a decision is made concerning the disclosure of any classified information. Decisions on the disclosure of classified military information are contingent on a decision by a principal or designated disclosure authority that the following criteria are met:

a. The disclosure supports U.S. foreign policy.

b. The release of classified military information will not have a negative impact on U.S. military security.

c. The foreign recipient has the capability and intent to protect the classified information.

d. There is a clearly defined benefit to the U.S. Government that outweighs the risks involved.

e. The release is limited to that classified information necessary to satisfy the U.S. Government objectives in authorizing the disclosure.

10-104. Bilateral Security Agreements. Bilateral security agreements are negotiated with various foreign governments. Confidentiality requested by some foreign governments prevents a listing of the countries that have executed these agreements.

a. The General Security Agreement, negotiated through diplomatic channels, requires that each government provide to the classified information provided by the other substantially the same degree of protection as the releasing government. The Agreement contains provisions concerning limits on the use of each government's information, including restrictions on third party transfers and proprietary rights. It does not commit governments to share classified information, nor does it constitute authority to release classified material to that government. It satisfies, in part, the eligibility requirements of the AECA concerning the agreement of the recipient foreign government to protect U.S. classified defense articles and technical data. (NOTE: The General Security Agreement also is known as a General Security of Information Agreement and General Security of Military Information Agreement. The title and scope are different, depending on the year the particular agreement was signed.)

b. Industrial security agreements have been negotiated with certain foreign governments which identify the procedures to be used when foreign government information is provided to industry. The Office of the Under Secretary of Defense (Policy) negotiates Industrial Security Agreements as an Annex to the General Security Agreement and the Director, Defense Investigative Service, has been delegated authority to implement the provisions of the Industrial Security Agreements. The Director of Security, NRC, negotiates and implements these agreements for the NRC.

Section 2. Disclosure of U.S. Information to Foreign Interests

10-200. General. Contractors shall avoid creating false impressions of the U.S. Government's readiness to authorize release of classified information to a foreign entity. If the information is derived from classified source material, is related to a classified GCA contract, and it has not been approved for public disclosure, advance disclosure authorization will be required. Disclosure authorization may be in the form of an export license, a letter authorization from the U.S. Government licensing authority, or an exemption to the export authorization requirements.

10-201. Authorization for Disclosure. Disclosure guidance will be provided by the GCA. Disclosure guidance provided for a previous contract or program shall not be used, unless the contractor is so instructed, in writing, by the GCA or the licensing authority. Classified information normally will be authorized for disclosure and export as listed below:

a. **Government-to-Government International Agreements.** Classified information shall not be disclosed until the agreement is signed by the participating governments and disclosure guidance and security arrangements are established. The export of technical data pursuant to such agreements may be exempt from ITAR licensing requirements.

b. **Symposia, Seminars, Exhibitions, and Conferences.** Appropriately cleared foreign nationals may participate in classified gatherings if authorized by the Head of the U.S. Government Agency that authorizes the conduct of the conference. All export controlled information to be disclosed shall be approved for disclosure pursuant to an export authorization or exemption covering the specific information and countries involved, or by written authorization from the designated disclosure authority of the originating Government Agency.

c. **Foreign Visits.** Disclosure of classified information shall be limited to that specific information authorized in connection with an approved visit request or export authorization.

d. **Sales, Loans, Leases, or Grants of Classified Items.** Disclosure of classified information or release of classified articles or services in connection with Government sales, loans, eases, or grants shall be in accordance with security arrangements specified by the GCA. Tests or demonstrations of U.S. classified articles prior to a purchase of inventory quantities of the item shall be under U.S. control unless an exception to policy is approved by the head of the GCA.

e. **Foreign Participation in Contractor Training Activities.** Disclosure of classified information to foreign nationals participating in training at contractor facilities shall be limited to information that is necessary for the operation and maintenance of, or training on, an item of equipment that has been sold to the trainee's government.

f. **Direct Commercial Sales.** The disclosure of classified information may be authorized pursuant to a direct commercial sale only if the proposed disclosure is in support of a U.S. or foreign government procurement requirement, a Government contract, or an international agreement. A direct commercial sale includes sales under a government agency sales financing program. If a proposed disclosure is in support of a foreign government requirement, the contractor should consult with U.S. in-country officials (normally the U.S. Security Assistance/Armaments Cooperation Office or Commercial Counselor).

g. **Temporary Exports.** Classified articles (including articles that require the use of classified information for operation) exported for demonstration purposes shall remain under U.S. control. The request for export authorization shall include a description of the arrangements that have been made in-country for U.S. control of the demonstrations and secure storage under U.S. Government control.

h. **Foreign Contractor Participation in U.S Classified Contracts.** Requests initiated by foreign contractors for classified information shall be submitted through the foreign country's embassy in Washington, DC, to the GCA foreign disclosure office. Approval of the request by GCA does not alleviate the requirement for a U.S. contractor to obtain an export authorization.

10-202. Direct Commercial Arrangements. An export authorization is required before a contractor makes a proposal to a foreign person that involves the eventual

disclosure of U.S. classified information. The contractor should obtain the concurrence of the GCA before submitting an export authorization request. To expedite disclosure and export decisions, the request for export authorization should include the following:

a. The U.S. or foreign government requirement that justifies the proposed export.

b. The type and classification level of any classified information and other export controlled technical information that ultimately would have to be exported, and the name, address, and telephone number of the Government entity that originated the classified information.

c. Identification of any prior licenses for the same articles or data.

d. A discussion of how U.S. operational and technology interests can be protected.

e. An evaluation of foreign availability of similar articles or technology.

f. The name, address, and telephone number of a U.S. and/or foreign government official who is knowledgeable concerning the government requirement.

g. The name, address, and telephone number of the CSA for U.S. contractors.

h. Any proposed security requirements that may require U.S. and/or foreign government approval.

i. Proposed transfer arrangements.

j. A Technology Control Plan (TCP), if applicable.

10-203. Retransfer and Security Assurances.

a. Requests for export authorizations that will involve the transfer of significant military equipment or classified material shall be accompanied by a Department of State Form DSP-83, Non-Transfer and Use Certificate. If classified material is involved, the form shall be signed by an official of the responsible foreign government who has the authority to certify that the transfer is for government purposes and that the classified material will be protected in compliance with a government-to-government security agreement.

b. If the transfer of classified material is not covered by a government-to-government agreement containing security requirements, an agreement will be necessary prior to the transfer of the material.

c. If a foreign government official refuses to sign the Form DSP-83, citing an existing agreement as the basis for refusal, that official should be requested to contact the Department of State, Office of Defense Controls, in writing, through its embassy in Washington, D.C. to address the requirement. The correspondence shall cite the existing agreement and certify that the material to be transferred is for government purposes and will be protected in compliance with the cited agreement.

10-204. Contract Security Requirements.

a. When a U.S. contractor is authorized to award a subcontract or enter into a Manufacturing License Agreement, Technical Assistance Agreement, or other direct commercial arrangement with a foreign contractor that will involve classified information, security requirements clauses will be incorporated in the subcontract document or agreement and security classification guidance via a Contract Security Classification Specification will be provided (see page 10-2-4). Two copies of the signed contract with the clauses and the classification guidance shall be provided to the CSA. If the export authorization specifies that additional security arrangements are necessary for performance on the contract, contractor developed arrangements shall be incorporated in appropriate clauses in the contract or in a separate security document.

b. The contractor shall prepare and maintain a written record that identifies the originator or source of classified information that will be used in providing defense articles or services to foreign customers. The contractor shall maintain this listing with the contractor's record copy of the pertinent export authorization.

Security Clauses for International Contracts

Security clauses, substantially as shown below, shall be included in all contracts and subcontracts involving classified information that are awarded to foreign contractors.

1. **All classified information and material furnished or generated pursuant to this contract shall be protected as follows:**

   a. **The recipient will not release the information or material to a third-country government, person, or firm without the prior approval of the releasing government.**

   b. **The recipient will afford the information and material a degree of protection equivalent to that afforded it by the releasing government; and**

   c. **The recipient will not use the information and material for other than the purpose for which it was furnished without the prior written consent of the releasing government.**

2. **Classified information and material furnished or generated pursuant to this contract shall be transferred through government channels or other channels specified in writing by the Governments of the United States and (insert applicable country) and only to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.**

3. **Classified information and material furnished under this contract will be remarked by the recipient with its government's equivalent security classification markings.**

4. **Classified information and material generated under this contract must be assigned a security classification as specified by the contract security classification specifications provided with this contract.**

5. **All cases in which it is known or there is reason to believe that classifed information or material furnished or generated pursuant to this contract has been lost or disclosed to unauthorized persons shall be reported promptly and fully by the contractor to its government's security authorities.**

6. **Classified information and material furnished or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:**

   a. **A potential contractor or subcontractor which is located in the United States or (insert applicable country) has been approved for access to classified information and material by U.S. or (insert applicable country) security authorities; or,**

   b. **If located in a third country, prior written consent is obtained from the United States Government.**

7. **Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be returned to the U.S. contractor or be destroyed.**

8. **The recipient contractor shall insert terms that substantially conform to the language of these clauses, including this clause, in all subcontracts under this contract that involve access to classified information furnished or generated under this contract.**

Section 3. Foreign Government Information

10-300. General. Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. This Section provides additional requirements for protecting and controlling access to foreign government information provided to U.S. contractors.

10-301. Policy. The contractor shall notify the CSA when awarded contracts by a foreign interest that will involve access to classified information. The CSA shall administer oversight and ensure implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material.

10-302. Marking Foreign Government Classified Material. Foreign government designations for classified information generally parallel U. S. security classification designations. However, some foreign governments have a fourth level of classification, RESTRICTED, for which there is no equivalent U.S. classification. The information is to be protected and marked as CONFIDENTIAL information. When other foreign government material is received, the equivalent U.S. classification and the country of origin shall be marked on the front and back in English. Foreign government classification designations and the U.S. equivalents are shown in Appendix B.

10-303. Marking U.S. Documents That Contain Foreign Government Information. U.S. documents that contain foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT (indicate level) INFORMATION." In addition, the portions shall be marked to identify the classification level and the country of origin, e.g., (UK-C); (GE-C). If a foreign government indicates that it does not want to be identified, applicable paragraphs shall be marked FGI together with the appropriate classification, e.g., (FGI-S). The "Classified by" line shall identify U.S. as well as foreign classification sources. If the foreign government does not want to be identified, a separate record shall be maintained. The "Declassify on" line shall contain the notation, "ORIGINATING AGENCY'S DETERMINATION REQUIRED" or "OADR." A U.S. document, marked as described herein, shall not be downgraded below the highest level of foreign government information contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted to the CSA.

10-304. Marking Documents Prepared For Foreign Governments. Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government. In addition, they shall be marked on the front, "THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION." Portions shall be marked to identify the U.S. classified information. The record specified in paragraph 10-204b shall be maintained.

10-305. PCL, FCL, and Briefing Requirements.

PCLs and FCLs issued by the U.S. Government are valid for access to classified foreign government information of a corresponding level. Contractor employees will be briefed and acknowledge in writing their responsibilities for handling foreign government information prior to being granted access.

10-306. Storage, Control, and Accountability. Foreign government material shall be stored and access controlled generally in the same manner as U.S. classified material of an equivalent classification. The procedures shall ensure that the material can be located at all times and access is limited to only those persons who require access for the specific purpose for which the information was provided by the originating government. Foreign government material shall be stored in a manner that will avoid commingling with other material which may be accomplished by establishing separate files in a storage container. Annual inventories are required for TOP SECRET and SECRET material.

10-307. Disclosure and Use Limitations. Foreign government information shall not be disclosed to nationals of a third country, including intending citizens, or to any other third party, or be used for other than the purpose for which it was provided, without the prior written consent of the originating foreign government. Requests for other uses or further disclosure shall be submitted to the GCA for U.S. contracts, and through the CSA for direct

commercial contracts. Approval of the request does not alleviate the requirement for the contractor to obtain an export authorization.

10-308. Exports of Foreign Government Information. An export authorization is required for the export or re-export of export-controlled foreign government information except for technical data being returned to the original source of import. All requests for export authorization for foreign government information shall clearly identify and distinguish between the foreign government information and any U.S. information involved in the same request. Foreign government information shall not be exported to a third party without the prior consent of the originating government. A copy of such consent shall be provided in writing to the Office of Defense Trade Controls, Department of State, with an information copy to the CSA.

10-309. Transfer. Foreign government information shall be transferred within the U.S., its possessions, or territories, using the same channels as specified by this Manual for U.S. classified information of an equivalent classification except that uncleared commercial delivery services shall not be used. The transfer of foreign government information to areas outside the U.S. shall be through government-to-government channels

10-310. Contract Security Requirements. The foreign entity that awards a classified contract is responsible for providing appropriate security classification guidance and any security requirements clauses. The failure of a foreign entity to provide classification guidance shall be reported to the CSA.

10-311. Public Disclosure. The public disclosure of foreign government information requires the prior written approval of the contracting foreign government.

10-312. Subcontracting.

a. A U.S. contractor may award a subcontract that involves access to foreign government information to another contractor within the U.S., its possessions or territories, except as described in subparagraph b, below, upon verifying with the CSA that the prospective subcontractor has the appropriate FCL and storage capability. The contractor awarding a subcontract shall provide appropriate security classification guidance and incorporate the pertinent security requirements clauses in the subcontract.

b. Subcontracts involving foreign government information shall not be awarded to a contractor in a third country or to a U.S. company with a limited FCL based on third-country ownership, control, or influence without the express written consent of the originating foreign government. The CSA will coordinate with the appropriate foreign government authorities to resolve the matter.

10-313. Reproduction. The reproduction of foreign government TOP SECRET information requires the written approval of the originating government. Reproduced copies of all foreign government information shall be controlled, protected, and accounted for in the same manner as the original version.

10-314. Disposition. Foreign government information shall be returned to the GCA or foreign government that provided the information, upon completion of the contract, unless the contract specifically authorizes destruction or retention of the information. TOP SECRET and SECRET destruction must be witnessed; destruction certificates are required for foreign government material and shall be retained for 3 years.

10-315. Loss, Compromise, or Suspected Compromise. The loss, compromise, or suspected compromise of foreign government material shall be reported promptly to the CSA.

10-316. Reporting of Improper Receipt of Foreign Government Material. The contractor shall report to the CSA the receipt of classified material from foreign interests that is not received through government channels.

10-317. Processing Foreign Government Classified Information on AISs. Foreign government information shall be processed on an AIS accredited to the appropriate classification level.

Section 4. International Transfers

10-400. General. This Section contains the procedures for international transfers of classified material. The requirements in this Section do not apply to the transmission of classified material to U.S. Government activities outside the United States. Copies of the forms, plans and certificates discussed in this Section may be obtained from the CSO.

10-401. Policy. All international transfers of classified material shall take place through government - to - government channels. Control and accountability of classified material must be maintained until the material is officially transferred to the intended recipient government through its designated government representative (DGR).

a. To ensure Government accountability, written transmission instructions shall be prepared for all international transfers of classified material. If the transfer involves the use of a commercial carrier or freight forwarder, the instructions shall be fully described in a Transportation Plan (TP). The instructions shall be approved by the CSA and the recipient government security authorities. Preparation of the instructions shall be the responsibility of: (1) The contractor for commercial contracts; and (2) The executing government agency for Government contracts.

b. In urgent situations, the CSA may authorize appropriately cleared contractor employees to handcarry classified material.

c. The CSA shall be contacted at the earliest possible stage in deliberations that will lead to the international transfer of classified material. The CSA shall advise the contractor on the transfer arrangements, identify the recipient government's DGR, appoint a U.S. government employee as the U.S. DGR, and ensure that the transportation plan prepared by the contractor or government is adequate.

10-402. Transfers of Freight.

a. **Government Agency Sales.** Classified material to be furnished to a foreign government under such transactions normally will be shipped via government agency-arranged transportation, such as the DTS, and be transferred to the foreign government's DGR within the recipient government's territory. In any Government Agency sales case, the Government Agency that executes the sale is responsible, in coordination with the recipient foreign government, for preparing a TP. When the point of origin is a U.S. contractor facility, the GCA shall provide the contractor and the applicable CSA a copy of the TP and the applicable Letter of Offer and Acceptance (LOA). If a freight forwarder is to be used in processing the shipment, the freight forwarder and its CSA also shall be provided a copy of the TP by the GCA.

b. **Commercial Contracts.** The contractor shall prepare a TP in coordination with the receiving government security officials. This requirement applies whether the material is to be moved by land, sea, or air, and applies to U.S. and foreign classified contracts. After the CSA approves the TP, it shall be forwarded to the recipient foreign government security authorities for final coordination and approval.

c. **Transportation Plan (TP).** A requirement to prepare a TP shall be included in each contract that involves the international transfer of classified material as freight. The TP shall describe arrangements for the secure shipment of the material from the point of origin to the ultimate destination. The U.S. and recipient government DGRs shall be identified in the TP. The TP shall provide for security arrangements in the event the transfer cannot be made promptly. When there are to be repetitive shipments, a Notice of Classified Consignment will be used. The shipment must be accompanied by an appropriately cleared escort.

d. **International Carriers.** The international transfer of classified material shall be made using only ships, aircraft, or other carriers that:

(1) Are owned or chartered by the U.S Government or under U.S. registry

(2) Are owned or chartered by or under the registry of the recipient government

(3) Are carriers other than those described that are expressly authorized to perform this function in writing by the Designated Security Authority of the GCA and the security authorities of the foreign government involved. This authority shall not be delegated and this

exception may be authorized only when a carrier described in (1) or (2), above, is not available and/or an urgent operational requirement dictates use of the exception.

10-404. Return of Material for Repair, Modification, or Maintenance. A foreign government or contractor may return classified material to a U.S. contractor for repair, modification, or maintenance. The approved methods of return shall be specified in either the GCA sales contract, the security requirements section of a direct commercial sales contract, or, in the case of material transferred as freight, in the original TP. The contractor, upon receipt of notification that classified material is to be received, will notify the applicable CSA. The CSA shall contact the applicable foreign government security officials and arrange for secure transportation within the United States.

10-405. Use of Freight Forwarders.

a. A commercial freight forwarder may be used to arrange for the international transfer of classified material as freight. The freight forwarder must be under contract to a Government Agency, U.S. contractor, or the recipient foreign government. The contract shall describe the specific functions to be performed by the freight forwarder. The responsibility for security and control of the classified material that is processed by freight forwarders remains with the U.S. Government until the freight is transferred to a DGR of the recipient government.

b. Only freight forwarders that have a valid FCL and storage capability at the appropriate level are eligible to take custody, or possession of classified material for delivery as freight to foreign recipients. Freight forwarders that only process unclassified paperwork and make arrangements for the delivery of classified material to foreign recipients do not require an FCL.

10-406. Handcarrying Classified Material. To meet an urgent need, the CSA may authorize contractor employees to handcarry classified material outside the United States. SECRET is the highest level of classified material to be carried and it shall be of such size and weight that the courier can retain it in his or her possession at all times. The CSA shall ensure that necessary arrangements are made with U.S. airport security and customs officials and that security authorities of the receiving government approve the plan. If the transfer is pursuant to a contract or a bilateral or multinational government program, the request shall be approved in writing by the GCA. The CSA shall be notified by the contractor of a requirement under this Section at least 5 work days in advance of the transfer. Furthermore:

a. The courier shall be a full-time, appropriately cleared employee of the dispatching contractor.

b. The courier shall be provided with a Courier Certificate that shall be consecutively numbered and be valid for one journey only. The journey may include more than one stop, if approved by the CSA and secure Government storage has been arranged at each stop. The Courier Certificate shall be returned to the dispatching security officer immediately upon completion of the journey.

c. Before commencement of each journey, the courier shall read and initial the Notes to the Courier attached to the Courier Certificate and sign the Courier Declaration . The Declaration shall be maintained by the FSO until completion of the next security inspection by the CSA.

d. The material shall be inventoried, and shall be wrapped and sealed in the presence of the U.S. DGR. The address of the receiving security office and the return address of the dispatching company security office shall be shown on the inner envelope or wrapping. The address of the receiving government's DGR shall be shown on the outer envelope or wrapping along with the return address of the dispatching office.

e. The dispatching company security office shall prepare three copies of a receipt based on the inventory, and list the classified material involved. One copy of the receipt shall be retained by the dispatching company security office and the other two copies shall be packed with the classified material. The security office shall obtain a receipt for the sealed package from the courier.

f. The dispatching company security office shall provide the receiving security office with 24 work hours advance notification of the anticipated date and time of the courier's arrival, and the identity of the courier. The receiving security office shall notify the dispatching company security office if the courier does not arrive within 8 hours of the expected time of

arrival. The dispatching security office shall notify its DGR of any delay, unless officially notified otherwise of a change in the courier's itinerary.

g. The receiving DGR shall verify the contents of the consignment and shall sign the receipts enclosed in the consignment. One copy shall be returned to the courier. Upon return, the courier shall provide the executed receipt to the dispatching security office.

h. Throughout the journey, the consignment shall remain under the direct personal control of the courier. It shall not be left unattended at any time during the journey, in the transport being used, in hotel rooms, in cloakrooms, or other such location, and it may not be deposited in hotel safes, luggage lockers, or in luggage offices. In addition, envelopes and packages containing the classified material shall not be opened en route, unless required by customs or other government officials.

i. When inspection by government officials is unavoidable, the courier shall request that the officials provide written verification that they have opened the package. The courier shall notify the FSO as soon as possible. The FSO shall notify the U.S. DGR. If the inspecting officials are not of the same country as the dispatching security office, the designated security authority in the country whose officials inspected the consignment also shall be notified by the CSA. Under no circumstances shall the classified consignment be handed over to customs or other officials for their custody.

j. When carrying classified material, the courier shall not travel by surface routes through third countries, except as authorized by the CSA. The courier shall travel only on carriers described in 10-403d, and travel direct routes between the U.S. and the destination.

10-407. Classified Material Receipts. There shall be a continuous chain of receipts to record international transfers of all classified material from the contractor through the U.S. DGR and the recipient DGR to the ultimate foreign recipient. The contractor shall retain an active suspense record until return of applicable receipts for the material. A copy of the external receipt that records the passing of custody of the package containing the classified material shall be retained by the contractor and each intermediate consignee in a suspense file until the receipt that is enclosed in the package is signed and returned. Follow-up action shall be initiated through the CSA if the signed receipt is not returned within 45 days. The contractor shall retain the receipt for 2 years.

10-408. Contractor Preparations for International Transfers Pursuant to Commercial and User Agency Sales. The contractor shall be responsible for the following preparations to facilitate international transfers:

a. Ensure that each party that will be involved in the transfer is identified in the applicable contract or agreement, and in the license application or letter request.

b. Notify the appropriate U.S. DGR when the material is ready.

c. Provide documentation or written certification by an empowered official (as defined in the ITAR) to the U.S. DGR to verify that the classified shipment is within the limitations of the pertinent export authorization or an authorized exemption to the export authorization requirements, or is within the limitations of the pertinent GCA contract.

d. Have the classified shipment ready for visual review and verification by the DGR. As a minimum this will include:

(1) Preparing the packaging materials, address labels, and receipts for review.

(2) Marking the contents with the appropriate U.S. classification or the equivalent foreign government classification, downgrading, and declassification markings, as applicable.

(3) Ensuring that shipping documents (including, as appropriate, the Shipper's Export Declaration) include the name and telephone number of the CSA that validates the license or letter authorization, and the FSO or his or her designee for the particular transfer.

(4) Have sent advance notification of the shipment to the CSA, the recipient, and to the freight forwarder, if applicable. The notification will require that the recipient confirm receipt of the shipment or provide notice to the contractor if the shipment is not received in accordance with the prescribed shipping schedule.

10-409. Transfers of Technical Data Pursuant to an ITAR Exemption.

a. The contractor shall provide to the DGR valid documentation (i.e., license, Letter of Offer and Acceptance, or agreement) to verify the export authorization for classified technical data to be transferred pursuant to an ITAR exemption. The documentation shall include a copy of the Form DSP-83 associated with the original export authorization.

b. Classified technical data to be exported pursuant to ITAR exemption 125.4(b)(1) shall be supported by a written authorization signed by a principal disclosure authority or designated disclosure authority of the Government Agency. A copy of the authorization shall be provided by the contractor through the CSA to the Office of Defense Trade Controls.

c. Exports shall not be permitted under a Manufacturing License or Technical Assistance Agreement for which the authorization has expired.

Section 5. International Visits and Control of Foreign Nationals

10-500. General. This Section describes the procedures that the United States and foreign governments have established to control international visits to their organizations and cleared contractor facilities. It also describes procedures for controlling access to sensitive areas and information by foreign national employees.

10-501. Policy.

a. All requests for international visits shall be processed in compliance with the requirements of this Section.

b. The contractor shall establish procedures to monitor international visits by their employees and visits or assignments to their facilities of foreign nationals to ensure that the disclosure of, and access to, export-controlled articles and related information are limited to those that are approved by an export authorization.

c. Visit authorizations shall not be used to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information; an export authorization is required for such situations.

10-502. Types and Purpose of International Visits.

Visit requests are necessary to make administrative arrangements, obtain security assurances, and disclosure decisions. There are three types of international visits.

a. **One-time Visits.** A visit for a single, short-term occasion (normally less than 30 days) for a specified purpose.

b. **Recurring Visits.** Intermittent, recurring visits over a specified period of time, normally up to 1 year in duration, in support of a Government-approved arrangement, such as an agreement, contract, or license. By agreement of the governments, the term of the authorization may be for the duration of the arrangement, subject to annual review, and validation.

c. **Extended Visits.** A single visit for an extended period of time, normally up to 1 year, in support of an agreement, contract, or license. (NOTE: Some governments have only two categories of visits (one-time and recurring) and refer to an extended visit as a one-time, long-term visit.)

10-503. Emergency Visits. Some foreign governments will accept a visit request submitted within 7 calendar days of the proposed visit for an "emergency visit." To qualify as an emergency visit, the visit must relate to a specific Government-approved contract, international agreement or announced request for proposal, and failure to make the visit reasonably could be expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity. Emergency visits are only approved as a single, one-time visit. The requester should coordinate the emergency visit in advance with the person to be visited and ensure that the complete name, grade or position, address, and telephone number of the person and a knowledgeable foreign government point of contact are provided in the visit request, along with the identification of the contract, agreement, or program and the justification for submission of the emergency visit request.

10-504. Requests for Recurring Visits. Recurring visit authorizations should be requested at the beginning of each program. After approval of the request, individual visits may be arranged directly with the security office of the location to be visited subject to three working days advance notice.

10-505. Amendments. Visit requests that have been approved or that are being processed may be amended only to change, add, or delete names and change dates. Amendments that request earlier dates than originally specified shall not be accepted. Emergency visit authorizations shall not be amended.

10-506. Visits Abroad by U.S. Contractors. Many foreign governments require the submission of a visit request for all visits to a government facility or a cleared contractor facility, even though classified information may not be involved. They also require that the requests be received a specified number of days in advance of the visit. These lead times for NATO countries are attached. An export authorization must be obtained if export controlled technical data is to be disclosed or if information to be divulged is related to a classified U.S. Government

program, unless the disclosure of the information is covered by an ITAR exemption. Visit request procedures are outlined as follows:

a. **Request Format.** The visit request format is contained on pages 10-5-4 and 10-5-5 and shall be forwarded to the CSA. The host for the visit should coordinate the visit in advance with appropriate government authorities who are required to approve the visit. It is the visitor's responsibility to ensure that such coordination has occurred.

b. **Government Agency Programs.** When contractor employees are to visit foreign government facilities or foreign contractors on U.S. Government orders in support of a Government contract or agreement, a visit request also shall be submitted by the contractor.

10-507. Visits by Foreign Nationals to U.S. Contractor Facilities. Requests for visits by foreign nationals to U.S. contractor facilities that will involve the disclosure of (a) U.S. classified information, (b) Unclassified information related to a U.S. Government classified program, or (c) Plant visits covered by Section 125.5 of the ITAR, shall be processed through the sponsoring foreign government (normally the visitor's embassy) to the U.S. Government Agency for approval. (NOTE: Requests for visits by foreign nationals that involve only commercial programs and related unclassified information may be submitted directly to the contractor. It is the contractor's responsibility to ensure that an export authorization is obtained, if applicable.) As described below, the U.S. Government Agency may approve or deny the request, or decline to render a decision.

a. **Government-Approved Visits.** U.S. Government-approved visits constitute an exemption to the export licensing provisions of the ITAR. U.S. Government approved visits shall not be used to avoid the export licensing requirements for commercial initiatives. When the cognizant U.S. Government Agency approves a visit, the notification of approval shall contain instructions on the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations. Final acceptance of the visit shall be subject to the concurrence of the contractor who shall notify the U.S. Government Agency when a visit is not desired.

b. **Visit Request Denials.** If the U.S. Government Agency does not approve the disclosure of the information related to the proposed visit, it will deny the visit request. The requesting government and the contractor to be visited shall be advised of the reason for the denial. The contractor may accept the visitor(s). However, only information that is in the public domain may be disclosed.

c. **Non-Sponsorship.** The U.S. Government Agency will decline to render a decision on a visit request that is not in support of a U.S. Government program. A declination notice, indicating that the visit is not Government approved (i.e., the visit is non-sponsored), shall be furnished to the requesting foreign government with an information copy to the U.S. contractor to be visited. A declination notice does not preclude the visit, provided the contractor has, or obtains, an export authorization for the information involved and, if classified information is involved, has been notified that the requesting foreign government has provided the required security assurance of the proposed visitor to the U.S. Government Agency in the original visit request. It shall be the responsibility of the contractor to consult applicable export regulations to determine licensing requirements regarding the disclosure of export controlled information during such visits by foreign nationals.

d. **Access by Foreign Visitors to Classified Information.** The contractor shall establish procedures to ensure that foreign visitors are not afforded access to classified information and other export-controlled technical data except as authorized by an export license, approved visit request, or other exemption to the licensing requirements. The contractor shall not inform the foreign visitor of the scope of access authorized or of the limitations imposed by the Government. Foreign visitors shall not be given custody of classified material except when they are acting as an official courier of their government and the CSA authorizes the transfer.

e. **Visitor Records.** Contractor visitor records shall clearly identify foreign visitors.

f. **Visits to Subsidiaries.** A visit request authorization for a visit to a parent facility also may be used for visits to other divisions or subsidiaries of the same company provided disclosures are for the same purpose, the information to be disclosed does not exceed the parameters of the approved visit request, and the U.S. Government Agency concurs.

10-508. Control of Access by On-Site Foreign Nationals

a. Extended visits and assignments of foreign nationals to contractor facilities shall be authorized only when it is essential that the foreign national be at the facility pursuant to a contract or Government agreement (e.g., joint venture, liaison representative to a joint or multinational program, or direct commercial sale).

b. If the foreign national will require access to export-controlled information related to, or derived from, a U.S. Government classified contract, the contractor shall obtain the written consent of the GCA prior to making a commitment to accept the proposed visit or assignment. A copy of the written consent shall be included with the request for export authorization, when such authorization is required.

c. The applicable CSA shall be notified in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities. The notification shall include a copy of the approved visit authorization or the U.S. Government export authorization, and the Technology Control Plan (TCP).

d. U.S. and foreign government classified material in a U.S. contractor facility is to remain under U.S. contractor custody and control and is subject to inspection by the FSO and the CSA. This does not preclude a foreign visitor from being furnished a security container for the temporary storage of classified material, consistent with the purpose of the visit or assignment, provided the CSA approves, and responsibility for the container and its contents remains with the U.S. contractor. Exceptions to this policy may be approved on a case-by-case basis by the CSA for the storage of foreign government classified information furnished to the visitor by the visitor's government through government channels. Exceptions shall be approved in advance, in writing, by the CSA, and agreed to by the visitor's government. The agreed procedures shall be included in the contractor's TCP, shall require the foreign nationals to provide receipts for the material, and shall include an arrangement for the CSA to ensure compliance, including provisions for the CSA to inspect and inventory the material.

10-509. TCP. A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the CSA determines that procedures already in place at the contractor's facility are adequate. The TCP shall contain procedures to control access for all export-controlled information. A sample of a TCP may be obtained from the CSA.

10-510. Security and Export Control Violations Involving Foreign Nationals. Any violation of administrative security procedures or export control regulations by foreign visitors or foreign national employees shall be reported to the CSA.

Standard Request For Visit Format

I. This matrix contains the instructions for the completion of a Request for Visit (RFV). The visit request must be submitted through the Facility Security Officer to the applicable Clearance Agency. The RFV format in Section II below, will be used for all requests for international visits as follows:

a. A separate request must be submitted for each program, project, or contract.

b. A separate request must be submitted for each country to be visited.

c. Subject to Government Agency restrictions, multiple locations may be listed for each country provided each location is involved in the same program, project, or contract.

d. The RFV may be locally produced on a form or form letter provided the specified format is followed. Information given to answer each data element must be typed or printed in block letters so that it is legible.

e. Most countries have established a specified number of working days that a visit request must be received for processing prior to the visit. The chart in Section III below, lists this information for the NATO member nations.

II. The RFV format will be completed in compliance with the format and instructions listed below. The Subject line of the request should state: Request for Visit Authorization - (insert name of country). The date of the request must be included in the heading. A reference should be made to any correspondence that supports the proposed visit, particularly if the reference includes an invitation.

1. **REQUESTING FACILITY.** Provide the full name and postal address (include city, state, country, and postal zone) and the name, organization, and telephone and telefax numbers of a person who is knowledgeable of the purpose of the visit.

2. **GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED.** Provide the full name and postal address (include city, state, country, and postal zone) and telefax and telephone number of the person with whom arrangements have been made for the visit at the facility.

(NOTE: An Annex should be used if more than two locations are to be visited. In such case, the statement. See also Annex ___ should be included.)

3. **DATES OF VISIT.** Provide the actual date or period (date-to-date) of the visit by day-month-year.

4. **TYPE OF VISIT.** Specify whether the visit is a government initiative or commercial initiative and whether the visit is being initiated by the requesting facility or the facility to be visited. Government initiative will be specified only if the visit is in support of an authorized government program, which must be fully described in item 7.

5. **SUBJECT TO BE DISCUSSED/JUSTIFICATION.** Give a concise description of the issues or subjects to be discussed and the reason for the visit. Do not use unexplained abbreviations. In the case of a request for recurring visits, this item should state Recurring Visits as the first words in the data element (e.g., Recurring Visits to discuss . . .).

6. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED.** Indicate SECRET, CONFIDENTIAL, RESTRICTED, or UNCLASSIFIED as applicable, and country of origin of the information.

7. **PERTINENCE OF VISIT.** Specify the full name of the government program, agreement, or sales contract (e.g., FMS case), or request for proposal or tender offer, using commonly used or explained abbreviations only.

8. **PARTICULARS OF VISITOR.**

NAME:	**Family name, followed by forename in full and middle initial(s).**
DOB:	**Date of birth (day-month-year).**
POB:	**Place of birth (city, state, and country).**
SC:	**Security clearance status (e.g., TS, S, C). Indicate NATO clearance if the visit is related to NATO business.**
ID-PP:	**Enter the passport number.**
NATIONALITY:	**Enter citizenship.**
POSITION:	**Provide the position the visitor holds in the organization (e.g., director, product manager, etc.)**
COMPANY? AGENCY	**Provide the name of the government agency or industrial facility that the visitor represents if different from item 1.**

NOTE: If more than 2 visitors are involved in the visit, a continuation sheet should be used. In that case item 8 should state "SEE ANNEX_, NUMBER OF VISITORS:. . . (state the number of visitors).

9. SECURITY OFFICER OF THE REQUESTING CONTRACTOR. Provide the name and telephone number of the requesting Facility Security Officer.

10. CERTIFICATION OF SECURITY CLEARANCE. Do not fill in (to be completed by the Government Clearance Agency).

NOTE: Item 10 also may be filled in by the appropriate official of the U.S. Embassy in the country to be visited or the applicable Office of Industrial Security International (OISI).

11. REMARKS.

(a) This item can be used for certain administrative requirements (e.g., proposed itinerary, request for hotel reservations, and/or transportation).

(b) In the case of an Emergency Visit, the name, telephone, and telefax numbers of the knowledgeable person with whom advance arrangements have been made should be stated.

III. Lead-times (i.e., the number of days in advance that the request must be received by the host government) for NATO nations are as follows:

	One-time and Recurring Visits	Amendments
Belgium	14	9
Canada	20	10
Denmark	7	5
France	25	5
Germany	25	10
Greece	20	10
Italy	14	7
Luxembourg	10	9
Netherlands	20	5
Norway	15	10
Portugal	20	7
Spain	25	8
Turkey	15	10
United Kingdom	21	5

Section 6. Contractor Operations Abroad

10-600. General. This Section sets forth requirements governing contractor operations abroad, including PCLs for U.S. contractor employees assigned outside the U.S. and their access to classified information.

10-601. Access by Contractor Employees Assigned Outside the United States.

a. Contractor employees assigned outside the United States, its possessions or territories may have access to classified information in connection with performance on a specified United States, NATO, or foreign government classified contract.

b. The assignment of an employee who is a foreign national, including intending citizens, outside the U.S. on programs that will involve access to classified information is prohibited and negates the basis on which an LAA may have been provided to such employee.

c. A consultant shall not be assigned outside the United States with responsibilities that require access to classified information.

10-602. Storage, Custody, and Control of Classified Information Abroad by Employees of a U.S. Contractor.

a. The storage, custody, and control of classified information required by a U.S. contractor employee abroad is the responsibility of the U.S. Government. Therefore, the storage of classified information by contractor employees at any location abroad that is not under U.S. Government control is prohibited. The storage may be at a U.S. military facility, a U.S. Embassy or Consulate, or other location occupied by a U.S. Government organization.

b. A contractor employee may be furnished a security container to temporarily store classified material at a U.S. Government Agency overseas location. The decision to permit a contractor to temporarily store classified information must be approved in writing by the senior security official for the U.S. Government host organization.

c. A contractor employee may be permitted to temporarily remove classified information from an overseas U.S. Government controlled facility, when necessary for the performance of a GCA contract or pursuant to an approved export authorization. The responsible U.S. Government security official at the U.S. Government facility shall verify that the contractor has an export authorization or other written U.S. Government approval to have the material; verify the need for the material to be removed from the facility; and brief the employee on handling procedures. In such cases, the contractor employee shall sign a receipt for the classified material. Arrangements shall also be made with the U.S. Government custodian for the return and storage of the classified material during non-duty hours. Violations of this policy shall be reported to the applicable CSA by the security office at the U.S. Government facility.

d. A contractor employee shall not store classified information at overseas divisions or subsidiaries of U.S. companies incorporated or located in a foreign country. (NOTE: The divisions or subsidiaries may possess classified information that has been transferred to the applicable foreign government through government-to-government channels pursuant to an approved export authorization or other written U.S. Government authorization. Access to this classified information at such locations by a U.S. contractor employee assigned abroad by the parent facility on a visit authorization in support of a foreign government contract or subcontract, is governed by the laws and regulations of the country in which the division or subsidiary is registered or incorporated. The division or subsidiary that has obtained the information from the foreign government shall provide the access.)

e. U.S. contractor employees assigned to foreign government or foreign contractor facilities under a direct commercial sales arrangement will be subject to the host-nation's industrial security policies.

10-603. Transmission of Classified Material to Employees Abroad. The transmission of classified material to a cleared contractor employee located outside the United States shall be through U.S. Government channels. If the material is to be used for other than U.S. Government purposes, an export authorization is required and a copy of the authorization, validated by the designated Government representative, shall accompany the material. The material shall be addressed to a U.S. military organization or other U.S. Government organization (e.g., an Embassy). The U.S. government organization abroad shall be responsible for custody and control of the material.

10-604. Security Briefings. An employee being assigned outside the United States shall be briefed on the security requirements of their assignment, including the handling, disclosure, and storage of classified information overseas.

10-605. Report of Assignments.

a. The contractor shall promptly report to the CSA the assignment of a cleared employee to a location outside the United States, Puerto Rico, Guam, or the Virgin Islands for a period exceeding 90 consecutive days. The report shall contain the following information:

(1) Name, address, telephone number, and CSA overseas code (if applicable) of the location to which the employee will be assigned; whether the location is under U.S. Government or foreign government control; and name, title, and telephone number of the U.S. Government or foreign government security official at the location.

(2) Justification for access to any U.S. or foreign government classified information, including identification of the contract, license, or agreement under which access is necessary.

b. Subsequent to the assignment of a cleared employee outside the United States, the contractor shall provide to the CSA:

(1) Justification, based on a specified contract, license, agreement, or other Government-approved arrangement, for the employee's continuing need for a PCL every 3 years following the initial assignment.

(2) Notification of any change in the location and mailing address of the affected employee.

(3) Notification of the termination of the employee's assignment outside the United States.

Section 7. NATO Information Security Requirements

10-700. General. This Section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO(USSAN) for safeguarding NATO information provided to U.S. industry.

10-701. Classification Levels. NATO has four levels of security classification; COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

10-702. NATO Contracts. NATO contracts involving NATO-unique systems, programs, or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO Management Agency, the NATO Research Staff, or a NATO Command. In the case of NATO infrastructure projects (e.g., airfields, communications), the NATO contract is awarded by a contracting agency or prime contractor of the NATO nation that is responsible for the infrastructure project.

10-703. NATO Facility Security Clearance Certificate. A NATO Facility Security Clearance Certificate (FSCC) is required for a contractor to negotiate or perform on a NATO classified contract A U.S. facility qualifies for a NATO FSCC if it has an equivalent U.S. FCL and its personnel have been briefed on NATO procedures. The CSA shall provide the NATO FSCC to the requesting activity. A NATO FSCC is not required for GCA contracts that involve access to NATO classified information.

10-704. FCL Requirements. Access to NATO classified information requires a final FCL at the equivalent level. A FCL is not required for access to NATO RESTRICTED information.

10-705. NATO Briefings. Prior to having access to NATO classified information including Restricted, employees shall be given a NATO security briefing that covers the requirements of this Section and the consequences of negligent handling of NATO classified information. The FSO shall be initially briefed by a representative of the CSA. Annual refresher briefings shall also be conducted. When access to NATO classified information is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information. Such certificates shall be maintained for 2 years for NATO SECRET, CONFIDENTIAL and RESTRICTED, and 3 years for COSMIC TOP SECRET and all ATOMAL information.

10-706. Access to NATO Classified Information by Foreign Nationals. Foreign nationals of non-NATO nations may have access to NATO classified information only with the consent of the NATO Office of Security and the contracting activity. Requests shall be submitted to the Central U.S. Registry (CUSR). Access to NATO classified information may be permitted for citizens of NATO member nations provided a NATO security clearance certificate is provided by their government and they have been briefed.

10-707. Subcontracting for NATO Contracts. The contractor shall obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued prior to awarding the subcontract. The request for approval will be forwarded through the CSA.

10-708. Preparing and Marking NATO Documents.

All classified documents created by a U.S. contractor shall be portion marked. Any portion extracted from a NATO document that is not portion marked, must be assigned the classification that is assigned to the NATO document.

a. All U.S. originated NATO classified documents shall bear an assigned reference number and date on the first page. The reference numbers shall be assigned as follows:

   (1) The first element shall be the abbreviation for the name of the contractor facility.

(2) The second element shall be the abbreviation for the overall classification followed by a hyphen and the four digit sequence number for the document within that classification that has been generated for the applicable calendar year.

(3) The third element is the year; e.g., MM/NS-0013/93.

b. COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall bear the reference number on each page and a copy number on the cover or first page. Copies of NATO documents shall be serially numbered. Pages shall be numbered. The first page or index or table of contents shall include a list, including page numbers, of all Annexes and Appendices. The total number of pages shall be stated on the first page. All Annexes or Appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

c. One of the following markings shall be applied to NATO documents that contain ATOMAL information:

(1) "This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly."

(2) "This document contains UK ATOMIC Information. This information is released to the North Atlantic Treaty Organization including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom."

d. Working papers shall be retained only until a final product is produced.

10-709. Classification Guidance. Classification guidance shall be in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification. If adequate classification guidance is not received, the contractor shall contact the CSA for assistance. NATO classified documents and NATO information in other documents shall not be declassified or downgraded without the prior written consent of the originating activity. Recommendations concerning the declassification or downgrading of NATO classified information shall be forwarded to the CUSR.

10-710. Further Distribution. The contractor shall not release or disclose NATO classified information to a third party or outside the contractor's facility for any purpose without the prior written approval of the contracting agency.

10-711. Storage of NATO Documents. NATO classified documents shall be stored as prescribed for U.S. documents of an equivalent classification level, except as described below.

a. NATO classified documents shall not be commingled with other documents. NATO RESTRICTED documents may be stored in locked filing cabinets, bookcases, desks, or other similar locked containers that will deter unauthorized access.

b. Combinations for containers used to store NATO classified information shall be changed annually. The combination also shall be changed when an individual with access to the container departs or no longer requires access to the container, and if the combination is suspected of being compromised.

c. When the combination is recorded it shall be marked with the highest classification level of documents stored in the container as well as to indicate the level and type of NATO documents in the container. The combination record must be logged and controlled in the same manner as NATO classified documents.

10-712. International Transmission. NATO has a registry system for the receipt and distribution of NATO documents within each NATO member nation. The central distribution point for the U.S. is the CUSR located in the Pentagon. The CUSR establishes subregistries at U.S. Government organizations for further distribution and control of NATO documents. Subregistries may establish control points and sub-control points at contractor facilities. COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents shall be transferred through the registry system. NATO CONFIDENTIAL and RESTRICTED documents provided as part of NATO infrastructure contracts shall be transmitted via

government-to-government channels in compliance with Section 4 of this Chapter.

10-713. Handcarrying. NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED documents may be handcarried across international borders if authorized by the GCA. The courier shall be issued a NATO Courier Certificate by the CSA. When handcarrying is authorized, the documents shall be delivered to a U.S. organization at NATO, which shall transfer them to the intended NATO recipient.

10-714. Reproduction. Reproductions of COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL information shall be performed by the responsible Registry. The reproduction of NATO SECRET, CONFIDENTIAL, and RESTRICTED documents may be authorized to meet contractual requirements unless reproduction is prohibited by the contracting entity. Copies of COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall be serially numbered and controlled and accounted for in the same manner as the original.

10-715. Disposition. Generally, all NATO classified documents shall be returned to the contracting activity that provided them, upon completion of the contract. Documents provided in connection with an invitation to bid also shall be immediately returned if the bid is not accepted or submitted. NATO classified documents may be destroyed when permitted by either the contract or invitation to bid COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents shall be destroyed by the Registry that provided the documents. Destruction of COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents shall be witnessed.

10-716. Accountability Records. Logs, receipts, and destruction certificates are required for NATO classified information, as described below. Records for NATO documents shall be maintained separately from records of non-NATO documents. COSMIC TOP SECRET and all ATOMAL documents shall be recorded on logs maintained separately from other NATO logs and be assigned unique serial control numbers. Additionally, disclosure records, bearing the name and signature of each person that has access, are required for all COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.

a. Minimum identifying data on logs, receipts, and destruction certificates shall include the NATO reference number, short title, date of the document, classification, and serial copy numbers. Logs shall reflect the short title, unclassified subject, and distribution of the documents.

b. Receipts are required for all NATO classified documents except NATO CONFIDENTIAL and RESTRICTED.

c. Inventories shall be conducted annually of all COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents.

d. Destruction certificates are required for all NATO classified documents except RESTRICTED. The destruction of COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be witnessed.

e. Records shall be retained for 10 years for COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents and 3 years for NATO SECRET, NATO SECRET ATOMAL, NATO CONFIDENTIAL, and NATO CONFIDENTIAL ATOMAL documents.

10-717. Security Violations and Loss, Compromise, or Possible Compromise. The contractor shall immediately report the loss, compromise, suspected loss or compromise, and security violations involving NATO classified information to the CSA.

10-718. Extracting from NATO Documents. Permission to extract from a COSMIC TOP SECRET or ATOMAL document shall be obtained from the CUSR.

a. If extracts of NATO information are included in a U.S. document prepared for a non-NATO contract, the document shall be marked with U.S. classification markings. The caveat, "THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION" also shall be marked on the front cover or first page,of the document. Additionally, each paragraph or portion containing the NATO information shall be marked with the appropriate NATO classification, abbreviated in parentheses (e.g., NS) preceding the portion or paragraph. The "Declassify on" line of the document shall show "Originating Agency Determination Required" or "OADR" unless

the original NATO document shows a specific date for declassification.

b. NATO RESTRICTED information may be included in U.S. unclassified documents. The U.S. document must be marked, "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." It shall be protected as NATO RESTRICTED information.

c. The declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO activity. Requests shall be submitted to the CUSR for NATO contracts, through the GCA for U.S. contracts, and through the CSA for non-NATO contracts awarded by a NATO member nation.

10-719. Release of U.S. Information to NATO.

a. The release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization. When a document containing U.S. classified information is being prepared for NATO, the appropriate NATO classification markings shall be applied to the document. Documents containing U.S. classified information, and U.S. classified documents that are authorized for release to NATO, shall be marked on the cover or first page "THIS DOCUMENT CONTAINS U.S. CLASSIFIED INFORMATION. THE INFORMATION IN THIS DOCUMENT HAS BEEN AUTHORIZED FOR RELEASE TO (cite the NATO organization) BY (cite the applicable license or other written authority.)" The CSA shall provide transmission instructions to the contractor. The material shall be addressed to a U.S. organization at NATO, which shall then place the material into NATO security channels. The material shall be accompanied by a letter to the U.S. organization that provides transfer instructions and assurances that the material has been authorized for release to NATO. The inner wrapper shall be addressed to the intended NATO recipient. Material to be sent to NATO via mail shall be routed through the U.S. Postal Service and U.S. military postal channels to the U.S. organization that will make the transfer.

b. A record shall be maintained that identifies the originator and source of classified information that are used in the preparation of documents for release to NATO. The record shall be provided with any request for release authorization.

10-720. Visits. NATO visits are visits by personnel representing a NATO entity and relating to NATO contracts and programs. NATO visits shall be handled in accordance with the requirements in Section 5 of this Chapter. A NATO Certificate of Security Clearance will be included with the visit request.

a. **NPLO and NATO Industrial Advisory Group (NIAG) Recurring Visits.** NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies that are participating in a NPLO or NIAG contract or program. The NATO Management Office or Agency responsible for the NPLO program will prepare a list of the Government and contractor facilities participating in the program. For NIAG programs, the list will be prepared by the responsible NATO staff element. The list will be forwarded to the appropriate clearance agency of the participating nations, which will forward it to the participating contractor.

b. **Visitor Record.** Contractor visitor records shall clearly identify NATO visitors including those by U.S. personnel assigned to NATO. The records shall be maintained for 3 years.